BUNDESREPUBLIK DEUTSCHLAND

#4

jc808 U.S. PTO
09/766102
01/19/01

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	100 02 203.0
Anmeldetag:	19. Januar 2000
Anmelder/Inhaber:	ROBERT BOSCH GMBH, Stuttgart/DE
Bezeichnung:	Verfahren zum Schutz eines Mikrorechner-Systems gegen Manipulation von in einer Speicheranordnung des Mikrorechner-Systems gespeicherten Daten
IPC:	G 06 F 12/14

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 23. November 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Waasmaier

EL302702849

A 9161
06/00
EDV-L

R. 37282

11.01.2000

Robert Bosch GmbH , 70469 Stuttgart

Verfahren zum Schutz eines Mikrorechner-Systems gegen Manipulation von in einer Speicheranordnung des Mikrorechner-Systems gespeicherten Daten

Stand der Technik

Die vorliegende Erfindung betrifft ein Verfahren zum Schutz eines Mikrorechner-Systems gegen Manipulation von in einer Speicheranordnung des Mikrorechner-System gespeicherten Daten. Die Erfindung betrifft insbesondere ein Verfahren zum Schutz eines in der Speicheranordnung gespeicherten Programms. Das Mikrorechner-System weist einen der Speicheranordnung zugeordneten Mikrorechner auf, der zur Abarbeitung der Daten bzw. des Programms auf die Speicheranordnung zugreift. Die Erfindung betrifft außerdem eine Speicheranordnung, in der Daten, insbesondere ein Programm, gespeichert sind und der mindestens ein Mikrorechner zugeordnet ist, der zur Abarbeitung der Daten bzw. des Programms auf die Speicheranordnung zugreift. Schließlich betrifft die Erfindung ein Mikrorechner-System mit mindestens einem Mikrorechner und einer dem oder jedem Mikrorechner zugeordneten Speicheranordnung, in der Daten, insbesondere ein Programm, gespeichert sind, wobei der oder jeder Mikrorechner zur Abarbeitung der Daten bzw. des Programms auf die Speicheranordnung zugreift.

Das Mikrorechner-System mit dem Mikrorechner und der Speicheranordnung bildet bspw. einen Teil eines

Steuergeräts für ein Kraftfahrzeug. Ein solches Steuergerät steuert unterschiedliche Funktionen in einem Kraftfahrzeug, bspw. die Brennkraftmaschine, das Getriebe, den Brems- und Antriebsstrang, die Fahrdynamikregelung u. a.. Das Steuergerät weist üblicherweise einen Mikrorechner mit einem internen nur-Lesespeicher und einem internen wiederbeschreibbaren Speicher auf. Ein Steuerprogramm des Steuergeräts ist zumindest teilweise in dem wiederbeschreibbaren Speicher gespeichert. Durch eine Umprogrammierung des Steuerprogramms ist es theoretisch möglich, die gesteuerten Funktionen in dem Kraftfahrzeug gezielt zu verändern. Durch eine Manipulation des Steuerprogramms für die Brennkraftmaschine lässt sich bspw. auf relativ einfache Weise eine Leistungssteigerung der Brennkraftmaschine erzielen (sog. Chip-Tuning). Dies geht jedoch häufig auf Kosten einer langen Lebensdauer und einer niedrigen Abgasemission der Brennkraftmaschine. Aus diesem Grund führt eine unautorisierte Umprogrammierung des Steuerprogramms eines Steuergeräts zum Ausschluss von Haftungs- und Gewährleistungsansprüchen.

Aus dem Stand der Technik sind verschiedene Verfahren zum Schutz von Mikrorechnern gegen eine Manipulation des Steuerprogramms und verschiedene geschützte Mikrorechner bekannt. In der DE 197 23 332 A1 wird das sog. Seed & Key-Verfahren beschrieben, das in der Praxis weit verbreitet ist. Bei diesem bekannten Verfahren wird ein Überprüfungsprogramm in dem internen nur-Lesespeicher des Mikrorechners gespeichert. Bei jedem Start des Mikrorechners wird das Überprüfungsprogramm ausgeführt, bei dem mit einem Schlüssel aus zumindest einem Teil des Speicherinhalts des wiederbeschreibbaren Speichers ein Codewort ermittelt und mit einem in dem wiederbeschreibbaren Speicher abgelegten Vergleichscodewort verglichen wird. Bei einer Übereinstimmung des Codeworts

mit dem Vergleichscodewort wird der Mikrorechner zur Ausführung weiterer Programme freigegeben. Anderenfalls wird der Mikrorechner zumindest teilweise gesperrt.

Wenn nun das Steuerprogramm des Mikrorechners manipuliert wird, wird zunächst der wiederbeschreibbare Speicher gelöscht und mit einem manipulierten Steuerprogramm überschrieben. Dabei geht auch das ursprünglich in dem wiederbeschreibbaren Speicher gespeicherte Vergleichscodewort verloren. Zur Generierung eines neuen Codeworts wird der Schlüssel benötigt, der jedoch nicht frei verfügbar ist. Deshalb stimmen nach einer Manipulation des Steuerprogramms in der Regel das Vergleichscodewort und das Codewort nicht überein und der Mikrorechner wird gesperrt.

Das aus dem Stand der Technik bekannte Seed & Key-Verfahren setzt jedoch einen Mikrorechner mit einem internen nur-Lesespeicher voraus, in dem das Überprüfungsprogramm gespeichert wird. Das bekannte Verfahren funktioniert nicht bei einem Mikrorechner, der nicht über einen internen Speicher verfügt.

Deshalb ist es Aufgabe der vorliegenden Erfindung, bei einem Mikrorechner, der nicht über einen internen Speicher verfügt, sondern auf eine externe Speicheranordnung zugreift, die Manipulation des Speicherinhalts, d. h. von in der Speicheranordnung gespeicherten Daten oder eines gespeicherten Programms, zu verhindern.

Zur Lösung dieser Aufgabe wird ausgehend von dem Verfahren zum Schutz eines Mikrorechner-Systems der eingangs genannten Art vorgeschlagen, dass vor dem Einsatz der Speicheranordnung dem oder jedem zugeordneten Mikrorechner oder der Speicheranordnung eine individuelle Kennung

zugewiesen wird, dass in Abhängigkeit der Kennung ein Vergleichscode generiert und in der Speicheranordnung gespeichert wird und dass vor oder während dem Betrieb des Mikrorechner-Systems in Abhängigkeit der Kennung ein Sicherheitscode generiert und mit dem Vergleichscode verglichen wird.

Vorteile der Erfindung

Vor dem Einsatz der Speicheranordnung wird jedem Mikrorechner eine individuelle Kennung zugewiesen. Alternativ oder zusätzlich kann auch der Speicheranordnung eine individuelle Kennung zugewiesen werden. Diese Kennung kann z. B. als Zufallszahl bei der Fertigung des Mikrorechners oder durch Brennen von Fuses beim Kunden eingestellt werden. Wenn das Programm in die Speicheranordnung programmiert wird, wird auch ein in Abhängigkeit der Kennung generierter Vergleichscode in den Speicher übertragen.

Vor oder während dem Betrieb des Mikrorechner-Systems wird in Abhängigkeit der Kennung des oder jeden Mikrorechners bzw. der Speicheranordnung ein Sicherheitscode generiert und mit dem Vergleichscode verglichen. Der Vergleich des Sicherheitscodes mit dem Vergleichscode kann durch die Speicheranordnung und/oder durch den Mikrorechner ausgeführt werden.

Wenn der Vergleich durch die Speicheranordnung ausgeführt wird, wird die Speicheranordnung gesperrt, falls der Sicherheitscode nicht mit dem Vergleichscode übereinstimmt. Eine Ausführung des in der Speicheranordnung gespeicherten Programms durch den Mikrorechner ist dann nicht möglich, da der Mikrorechner nicht auf das Programm zugreifen kann.

Wenn der Vergleich durch den Mikrorechner ausgeführt wird, wird der Mikrorechner, falls der Sicherheitscode nicht mit dem Vergleichscode übereinstimmt, derart gesperrt, dass eine Ausführung des in der Speicheranordnung gespeicherten Programms nicht möglich ist.

Im Rahmen einer Manipulation von in der Speicheranordnung gespeicherten Daten, wird zunächst die Speicheranordnung gelöscht und dann mit manipulierten Daten überschrieben. Durch das Löschen der Speicheranordnung wird auch der Vergleichscode gelöscht und muss erneut in die Speicheranordnung geschrieben werden. Da die Kennung des oder jeden zugeordneten Mikrorechners bzw. die Kennung der Speicheranordnung jedoch nicht frei zugänglich ist, kann davon ausgegangen werden, dass der Sicherheitscode nach der Manipulation der Daten nicht mit dem Vergleichscode übereinstimmt.

Die heutige Gehäusetechnik von Mikrorechnern und Speicheranordnungen (z. B. Ball-Grid-Array (BGA)-Gehäuse) lässt es nur unter extremem Aufwand zu, die Kommunikation zwischen dem Mikrorechner und der Speicheranordnung nach einem Rücksetzen abzuhören, um auf diese Weise die Kennung des oder jeden Mikrorechners bzw. der Speicheranordnung in Erfahrung zu bringen. Selbst wenn es einer unbefugten Person auf diese Weise gelänge, die Kennung zu ermitteln, könnten mit Hilfe dieser Kennung lediglich die Daten dieser einen Speicheranordnung manipuliert werden. Eine Übertragung auf andere Mikrorechner-Systeme ist nicht möglich, da die Speicheranordnung oder der Mikrorechner anderer Mikrorechner-Systeme eine andere Kennung aufweist.

Erfindungsgemäß erfolgt also eine individuelle Zuordnung von Speicheranordnung und Mikrorechner eines Mikrorechner-Systems. Diese Zuordnung bewirkt, dass eine bestimmte

Speicheranordnung nur mit einem oder mehreren bestimmten zugeordneten Mikrorechnern zuverlässig zusammenarbeitet. Das Auslesen des Speichers, seine Modifikation und seine Duplizierung zum Zwecke der Manipulation der gespeicherten Daten ohne Kenntnis der individuellen Kennung des Mikrorechners oder der Speicheranordnung ist damit sinnlos.

Gemäß einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird vorgeschlagen, dass vor dem Einsatz der Speicheranordnung die individuelle Kennung als Vergleichscode in der Speicheranordnung gespeichert wird und dass vor oder während dem Betrieb der Speicheranordnung überprüft wird, ob der Vergleichscode mit der als Sicherheitscode verwendeten Kennung des oder jeden zugeordneten Mikrorechners übereinstimmt. Diese Weiterbildung stellt eine wesentliche Vereinfachung des erfindungsgemäßen Verfahrens dar, ohne dass dadurch der Schutz der Speicheranordnung vor Manipulation des Programms beeinträchtigt wird.

Wenn der Vergleich des Sicherheitscodes mit dem Vergleichscode durch die Speicheranordnung ausgeführt wird, arbeitet vorteilhafterweise die Speicheranordnung mit dem oder jedem Mikrorechner nur dann ordnungsgemäß zusammen, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt. Anderenfalls wird die Speicheranordnung gesperrt, und der Mikrorechner kann nicht auf das in der Speicheranordnung gespeicherte Programm zugreifen bzw. das Programm kann nicht aus der Speicheranordnung ausgelesen werden.

Wenn der Vergleich des Sicherheitscodes mit dem Vergleichscode alternativ oder zusätzlich durch den Mikrorechner ausgeführt wird, arbeitet der Mikrorechner nur mit der Speicheranordnung zusammen, falls der

Sicherheitscode mit dem Vergleichscode übereinstimmt. Anderenfalls wird der Mikrorechner derart gesperrt, dass eine Ausführung des in der Speicheranordnung gespeicherten Programms nicht möglich ist. Bei dieser Ausführungsform der Erfindung ist der Austausch der Speicheranordnung nicht möglich. Dies ist von besonderer Bedeutung, da es sonst für eine Person mit Manipulationsabsichten möglich wäre eine Speicheranordnung mit Schutzmerkmal gegen eine entsprechende Speicheranordnung ohne Schutzmerkmal auszustauschen. Um bei dieser Ausführungsform rein theoretisch eine Manipulation von in der Speicheranordnung gespeicherten Daten durchführen zu können, müsste sowohl der Mikrorechner als auch die Speicheranordnung gegen entsprechende Bauteile ohne Schutzmerkmale ausgetauscht werden. Das ist jedoch mit einem enormen Aufwand verbunden und wird deshalb in der Praxis kaum eine Rolle spielen.

Gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung wird vorgeschlagen, dass der Sicherheitscode vor dem Betrieb der Speicheranordnung nach jedem Hochfahren der Speicheranordnung generiert und mit dem Vergleichscode verglichen wird. Die Speicheranordnung ist vorzugsweise als ein Flash-Speicher ausgebildet.

Vorteilhafterweise wird die Speicheranordnung in einen Modus versetzt, in dem sie nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand geschaltet wird, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt. Nach dem Rücksetzen der Speicheranordnung kann diese nur durch eine bestimmte Aufschlusssequenz aktiviert werden. Die Aufschlusssequenz wird nur dann erzeugt, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt. Falls die Speicheranordnung diese Aufschlusssequenz nach einem Rücksetzen nicht sieht, so bleibt die Speicheranordnung in einem inaktiven Zustand.

Alternativ oder zusätzlich wird vorgeschlagen, dass der Mikrorechner in einen Modus versetzt wird, in dem er nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand geschaltet wird, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt. Nach dem Rücksetzen des Mikrorechners kann dieser nur durch eine bestimmte Aufschlusssequenz aktiviert werden. Die Aufschlusssequenz wird nur dann erzeugt, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt. Falls der Mikrorechner diese Aufschlusssequenz nach einem Rücksetzen nicht sieht, so bleibt er in einem inaktiven Zustand.

Das erfindungsgemäße Verfahren kann bei Mikrorechnern ohne internen Speicher eingesetzt werden. Selbstverständlich kann es aber auch bei Mikrorechnern eingesetzt werden, die über einen internen Speicher verfügen. Derartige Mikrorechner können außer durch das erfindungsgemäße Verfahren zusätzlich noch durch aus dem Stand der Technik bekannte Verfahren vor einer Manipulation des Programms geschützt werden. Deshalb wird gemäß einer anderen vorteilhaften Weiterbildung der vorliegenden Erfindung vorgeschlagen, dass ein in einem nur-Lesespeicher des Mikrorechners gespeichertes Überprüfungsprogramm ausgeführt wird, bei dem mit einem Schlüssel aus zumindest einem Teil des Speicherinhalts der Speicheranordnung ein Codewort ermittelt und mit einem in der Speicheranordnung abgelegten Vergleichscodewort verglichen wird. Gemäß dieser Weiterbildung wird der Mikrorechner zusätzlich noch durch das sog. Seed & Key-Verfahren vor einer Manipulation des Programms geschützt. Beide Verfahren zusammen ergeben bei Mikrorechnern, die über einen internen Speicher verfügen einen besonders wirksamen Schutz vor Manipulation.

Zur Lösung der Aufgabe der vorliegenden Erfindung wird des

Weiteren ausgehend von einer Speicheranordnung der eingangs genannten Art vorgeschlagen, dass in der Speicheranordnung ein in Abhängigkeit von einer dem oder jedem Mikrorechner und/oder der Speicheranordnung zugewiesenen individuellen Kennung generierter Vergleichscode gespeichert ist, und dass die Speicheranordnung Mittel aufweist, um vor oder während dem Betrieb des Mikrorechner-Systems in Abhängigkeit der individuellen Kennung einen Sicherheitscode zu generieren und mit dem Vergleichscode zu vergleichen.

Gemäß einer vorteilhaften Weiterbildung der Erfindung wird vorgeschlagen, dass die Speicheranordnung in einen Modus versetzbar ist, in dem sie nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand schaltet, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt.

Die Speicheranordnung ist vorteilhafterweise als ein Flash-Speicher, insbesondere als ein Flash Erasable Programmable Read Only Memory (Flash-EPROM) ausgebildet.

Zur Lösung der Aufgabe der vorliegenden Erfindung wird schließlich ausgehend von einem Mikrorechner-System der eingangs genannten Art vorgeschlagen, dass in der Speicheranordnung ein in Abhängigkeit von einer dem Mikrorechner oder der Speicheranordnung zugewiesenen individuellen Kennung generierter Vergleichscode gespeichert ist, und dass der Mikrorechner Mittel aufweist, um vor oder während dem Betrieb des Mikrorechner-Systems in Abhängigkeit der individuellen Kennung einen Sicherheitscode zu generieren und mit dem Vergleichscode zu vergleichen.

Gemäß einer vorteilhaften Weiterbildung der Erfindung wird vorgeschlagen, dass der Mikrorechner in einen Modus

versetzbar ist, in dem er nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand schaltet, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt.

Zeichnung

Eine bevorzugte Ausführungsform der vorliegenden Erfindung wird im Folgenden anhand der Zeichnungen näher erläutert. Es zeigt:

Fig. 1 ein Ablaufdiagramm des erfindungsgemäßen Verfahrens gemäß einer bevorzugten Ausführungsform; und

Fig. 2 ein erfindungsgemäßes Mikrorechner-System gemäß einer bevorzugen Ausführungsform.

Beschreibung der Ausführungsbeispiele

In Fig. 1 ist ein Ablaufdiagramm des erfindungsgemäßen Verfahrens gemäß einer bevorzugten Ausführungsform dargestellt. Das Verfahren dient zum Schutz eines Mikrorechner-Systems gegen Manipulation von in der Speicheranordnung gespeicherten Daten, insbesondere zum Schutz gegen Manipulation eines gespeicherten Programms. Der Speicheranordnung ist ein Mikrorechner zugeordnet, der zur Abarbeitung des Programms auf die Speicheranordnung zugreift. Ein solches Verfahren kann bspw. zum Schutz eines Steuergeräts eines Kraftfahrzeugs vor Manipulation des Steuerprogramms eingesetzt werden.

Das Verfahren beginnt in einem Funktionsblock 10. Dann wird in einem Funktionsblock 11 dem Mikrorechner, der der Speicheranordnung zugeordnet ist, eine individuelle Kennung zugewiesen. Die Kennung kann zufällig oder gezielt gewählt

werden. In einem nachfolgenden Funktionsblock 12 wird in Abhängigkeit der Kennung des Mikrorechners ein Vergleichscode generiert und in Funktionsblock 13 dann in der Speicheranordnung gespeichert. Im einfachsten Fall besteht der Vergleichscode aus der Kennung des Mikrorechners. Die Schritte 10 bis 13 werden vor dem Einsatz der Speicheranordnung, bspw. im Rahmen der Fertigung, ausgeführt.

Anschließend wird dann vor oder während dem Betrieb des Mikrorechner-Systems, bspw. nach jedem Hochfahren des Mikrorechner-Systems, in Funktionsblock 14 ein Sicherheitscode in Abhängigkeit der Kennung des Mikrorechners generiert. Im einfachsten Fall besteht der Sicherheitscode aus der Kennung des Mikrorechners. In einem nachfolgenden Abfrageblock 15 wird dann der Sicherheitscode in dem Mikrorechner mit dem Vergleichscode verglichen. Dazu findet eine Kommunikation zwischen dem Mikrorechner und der Speicheranordnung statt, in deren Verlauf der in der Speicheranordnung gespeicherte Vergleichscode von dem Mikrorechner gelesen wird. Falls der Sicherheitscode und der Vergleichscode übereinstimmen (ja), wird der Mikrorechner in Funktionsblock 16 freigegeben.

Nach dem Funktionsblock 16 findet außerdem eine Kommunikation zwischen dem Mikrorechner und der Speicheranordnung statt, in deren Verlauf der Sicherheitscode von dem Mikrorechner an die Speicheranordnung übertragen wird. In einem nachfolgenden Abfrageblock 17 wird dann der Sicherheitscode in der Speicheranordnung mit dem gespeicherten Vergleichscode verglichen. Falls der Sicherheitscode und der Vergleichscode übereinstimmen (ja), wird die Speicheranordnung in Funktionsblock 18 freigegeben. Das Steuergerät kann ganz normal seine Steuerungs- und Regelungsaufgaben erfüllen. Wenn die Speicheranordnung

erneut hochgefahren wird (gestrichelte Linie), beginnt das erfindungsgemäße Verfahren wieder bei Funktionsblock 14. Die Speicheranordnung wird bspw. durch ein Reset (Funktionsblock 22) zurückgesetzt und anschließend wieder hochgefahren.

Für die vorliegende Erfindung entscheidend ist, dass eine individuelle Zuordnung von Speicheranordnung und Mikrorechner des Mikrorechner-Systems erfolgt. Dies kann, wie oben beschrieben, durch eine Kennung des oder der Mikrorechner des Mikrorechner-Systems erfolgen. Alternativ oder zusätzlich kann das erfindungsgemäße Verfahren aber auch mit einer individuellen Kennung der Speicheranordnung arbeiten, durch die ebenfalls eine individuelle Zuordnung von Speicheranordnung und Mikrorechner erfolgen kann.

Falls der Sicherheitscode und der Vergleichscode nicht übereinstimmen (nein) wird der Mikrorechner in Funktionsblock 19 und/oder die Speicheranordnung in Funktionsblock 20 gesperrt. Dadurch wird das Auslesen bzw. das Ausführen des in der Speicheranordnung gespeicherten Programms verhindert. Das Steuergerät kann seine Steuerungs- und Regelungsfunktion nicht erfüllen. In Funktionsblock 21 ist das erfindungsgemäße Verfahren beendet.

Der Sicherheitscode stimmt bspw. dann nicht mit dem Vergleichscode überein, wenn die in der Speicheranordnung gespeicherten Daten manipuliert wurden und der Vergleichscode falsch oder gar nicht in der Speicheranordnung gespeichert wurde. Da die Kennung des Mikrorechners nur autorisierten Personen zur Verfügung steht, kann eine Änderung der Daten in der Speicheranordnung auch nur von diesen autorisierten Personen durchgeführt werden. Sie kennen die Kennung des

der Speicheranordnung zugeordneten Mikrorechners und können nach einer Änderung des Programms den richtigen Vergleichscode ermitteln und in der Speicheranordnung ablegen.

In Fig. 2 ist ein erfindungsgemäßes Mikrorechner-System gemäß einer bevorzugen Ausführungsform in ihrer Gesamtheit mit den Bezugszeichen 30 (Speicheranordnung) und 33 (Mikrorechner) bezeichnet. Die Speicheranordnung 30 weist einen wiederbeschreibbaren Speicher 31 auf, in dem zumindest ein Teil eines Programms gespeichert ist. Der Mikrorechner 33 greift mit seinem Mikrorechner-Kern 35 zur Abarbeitung des Programms auf den Speicher 31 zu. Der Mikrorechner 33 und die Speicheranordnung 30 sind bspw. Teil eines Steuergeräts für ein Kraftfahrzeug.

In dem Speicher 31 der Speicheranordnung 30 ist ein Vergleichscode gespeichert, der in Abhängigkeit von einer dem Mikrorechner 33 zugewiesenen individuellen Kennung generiert worden ist. Im einfachsten Fall kann der Vergleichscode die Kennung selbst sein. Vor oder während des Betriebs des Mikrorechner-Systems 30, 33, bspw. nach dem Hochfahren des Mikrorechner-Systems 30, 33, wird die Kennung des Mikrorechners 33 an die Speicheranordnung 30 übertragen. Die Speicheranordnung 30 weist Mittel 32 auf, um vor oder während dem Betrieb der Speicheranordnung 30 in Abhängigkeit der Kennung des Mikrorechners 33 den Sicherheitscode zu generieren. Im einfachsten Fall kann der Sicherheitscode die Kennung selbst sein.

Die Mittel 32, 34 vergleichen den Sicherheitscode mit dem gespeicherten Vergleichscode. Die Speicheranordnung 30 wird in einen Modus versetzt, in dem sie nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand geschaltet wird, wenn der Sicherheitscode mit dem

Vergleichscode übereinstimmt (Funktionsblock 18). Nach dem Rücksetzen der Speicheranordnung 30 kann diese nur durch eine bestimmte Aufschlusssequenz aktiviert werden. Die Aufschlusssequenz wird nur dann erzeugt, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt. Falls die Speicheranordnung 30 diese Aufschlusssequenz nach einem Rücksetzen nicht sieht, so bleibt sie in einem inaktiven Zustand (Funktionsblock 20).

Analog hierzu weist der Mikrorechner 33 Mittel 34 auf, um einen Sicherheitscode zu generieren und zu überprüfen. Der Mikrorechner 33 wird in einen Modus versetzt, in dem er nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand umschaltet, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt (Funktionsblock 16). Nach dem Rücksetzen des Mikrorechners 33 kann dieser nur durch eine bestimmte Aufschlusssequenz aktiviert werden. Die Aufschlusssequenz wird nur dann erzeugt, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt. Falls der Mikrorechner 33 diese Aufschlusssequenz nach einem Rücksetzen nicht sieht, so bleibt er in einem inaktiven Zustand (Funktionsblock 19).

Die Mittel 34 des Mikrorechners 33 überprüfen also die korrekte Identifiaktion der Speicheranordnung 30, die Mittel 32 der Speicheranordnung 30 überprüfen die korrekte Identifikation des Mikrorechners 33.

11.01.2000
Robert Bosch GmbH , 70469 Stuttgart

Ansprüche

1. Verfahren zum Schutz eines Mikrorechner-Systems (20, 23) gegen Manipulation von in einer Speicheranordnung (20) des Mikrorechner-System (20, 23) gespeicherten Daten, insbesondere zum Schutz eines in der Speicheranordnung (20) gespeicherten Programms, wobei das Mikrorechner-System (20, 23) einen der Speicheranordnung (20) zugeordneten Mikrorechner (23) aufweist, der zur Abarbeitung der Daten bzw. des Programms auf die Speicheranordnung (20) zugreift, **dadurch gekennzeichnet**, dass vor dem Einsatz der Speicheranordnung (20) dem oder jedem zugeordneten Mikrorechner (23) oder der Speicheranordnung (20) eine individuelle Kennung zugewiesen wird, dass in Abhängigkeit der individuellen Kennung ein Vergleichscode generiert und in der Speicheranordnung (20) gespeichert wird und dass vor oder während dem Betrieb des Mikrorechner-Systems (20, 23) in Abhängigkeit der individuellen Kennung ein Sicherheitscode generiert und mit dem Vergleichscode verglichen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass vor dem Einsatz der Speicheranordnung (20) die individuelle Kennung als Vergleichscode in der Speicheranordnung (20) gespeichert wird und dass vor oder während dem Betrieb des Mikrorechner-Systems (20, 23) überprüft wird, ob der Vergleichscode mit der als Sicherheitscode verwendeten Kennung des oder jeden

zugeordneten Mikrorechners (23) übereinstimmt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Speicheranordnung (20) mit dem oder jedem Mikrorechner (23) nur dann ordnungsgemäß zusammenarbeitet, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Sicherheitscode vor dem Betrieb der Speicheranordnung (20) nach jedem Hochfahren der Speicheranordnung (20) generiert und mit dem Vergleichscode verglichen wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Speicheranordnung (20) in einen Modus versetzt wird, in dem sie nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand geschaltet wird, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass der Mikrorechner (23) in einen Modus versetzt wird, in dem er nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand geschaltet wird, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass ein in einem nur-Lesespeicher des Mikrorechners (23) gespeichertes Überprüfungsprogramm ausgeführt wird, bei dem mit einem Schlüssel aus zumindest einem Teil des Speicherinhalts der Speicheranordnung (20) ein Codewort ermittelt und mit einem in der Speicheranordnung (20) abgelegten Vergleichscodewort verglichen wird.

8. Speicheranordnung (20), in der Daten, insbesondere ein Programm, gespeichert sind und der mindestens ein Mikrorechner (23) zugeordnet ist, der zur Abarbeitung der Daten bzw. des Programms auf die Speicheranordnung (20) zugreift, **dadurch gekennzeichnet**, dass in der Speicheranordnung (20) ein in Abhängigkeit von einer dem oder jedem Mikrorechner (23) oder der Speicheranordnung (20) zugewiesenen individuellen Kennung generierter Vergleichscode gespeichert ist, und dass die Speicheranordnung (20) Mittel (22) aufweist, um vor oder während dem Betrieb der Speicheranordnung (20) in Abhängigkeit der individuellen Kennung einen Sicherheitscode zu generieren und mit dem Vergleichscode zu vergleichen.

9. Speicheranordnung (20) nach Anspruch 8, dadurch gekennzeichnet, dass die Speicheranordnung (20) in einen Modus versetzbar ist, in dem sie nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand schaltet, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt.

10. Speicheranordnung (20) nach Anspruch 8 oder 9, dadurch gekennzeichnet, dass die Speicheranordnung (20) als ein Flash-Speicher ausgebildet ist.

11. Mikrorechner-System (20, 23) mit einem Mikrorechner (23) und einer dem Mikrorechner (23) zugeordneten Speicheranordnung (20), in der Daten, insbesondere ein Programm, gespeichert sind, wobei der Mikrorechner (23) zur Abarbeitung der Daten bzw. des Programms auf die Speicheranordnung (20) zugreift, **dadurch gekennzeichnet**, dass in der Speicheranordnung (20) ein in Abhängigkeit von einer dem Mikrorechner (23) oder der Speicheranordnung (20)

zugewiesenen individuellen Kennung generierter Vergleichscode gespeichert ist, und dass der Mikrorechner (23) Mittel (24) aufweist, um vor oder während dem Betrieb des Mikrorechner-Systems (20, 23) in Abhängigkeit der individuellen Kennung einen Sicherheitscode zu generieren und mit dem Vergleichscode zu vergleichen.

12. Mikrorechner (23) nach Anspruch 11, dadurch gekennzeichnet, dass der Mikrorechner (23) in einen Modus versetzbar ist, in dem er nach jedem Hochfahren nur dann aus einem inaktiven in einen aktiven Zustand schaltet, wenn der Sicherheitscode mit dem Vergleichscode übereinstimmt.

11.01.2000
Robert Bosch GmbH , 70469 Stuttgart

Verfahren zum Schutz einer Speicheranordnung gegen Manipulation eines in der Speicheranordnung gespeicherten Programms

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Schutz eines Mikrorechner-Systems (20, 23) gegen Manipulation von in einer Speicheranordnung (20) des Mikrorechner-System (20, 23) gespeicherten Daten, insbesondere zum Schutz eines in der Speicheranordnung (20) gespeicherten Programms, wobei das Mikrorechner-System (20, 23) einen der Speicheranordnung (20) zugeordneten Mikrorechner (23) aufweist, der zur Abarbeitung der Daten bzw. des Programms auf die Speicheranordnung (20) zugreift. Um bei einem Mikrorechner (23), der nicht über einen internen Speicher verfügt, sondern auf eine externe Speicheranordnung (20) zugreift und darin gespeicherte Daten abarbeitet, die Manipulation der Daten zu verhindern wird vorgeschlagen, dass vor dem Einsatz der Speicheranordnung (20) dem oder jedem zugeordneten Mikrorechner (23) oder der Speicheranordnung (20) eine individuelle Kennung zugewiesen wird, dass in Abhängigkeit der individuellen Kennung ein Vergleichscode generiert und in der Speicheranordnung (20) gespeichert wird und dass vor oder während dem Betrieb des Mikrorechner-Systems (20, 23) in Abhängigkeit der individuellen Kennung ein Sicherheitscode generiert und mit dem Vergleichscode verglichen wird. (Figur 2)

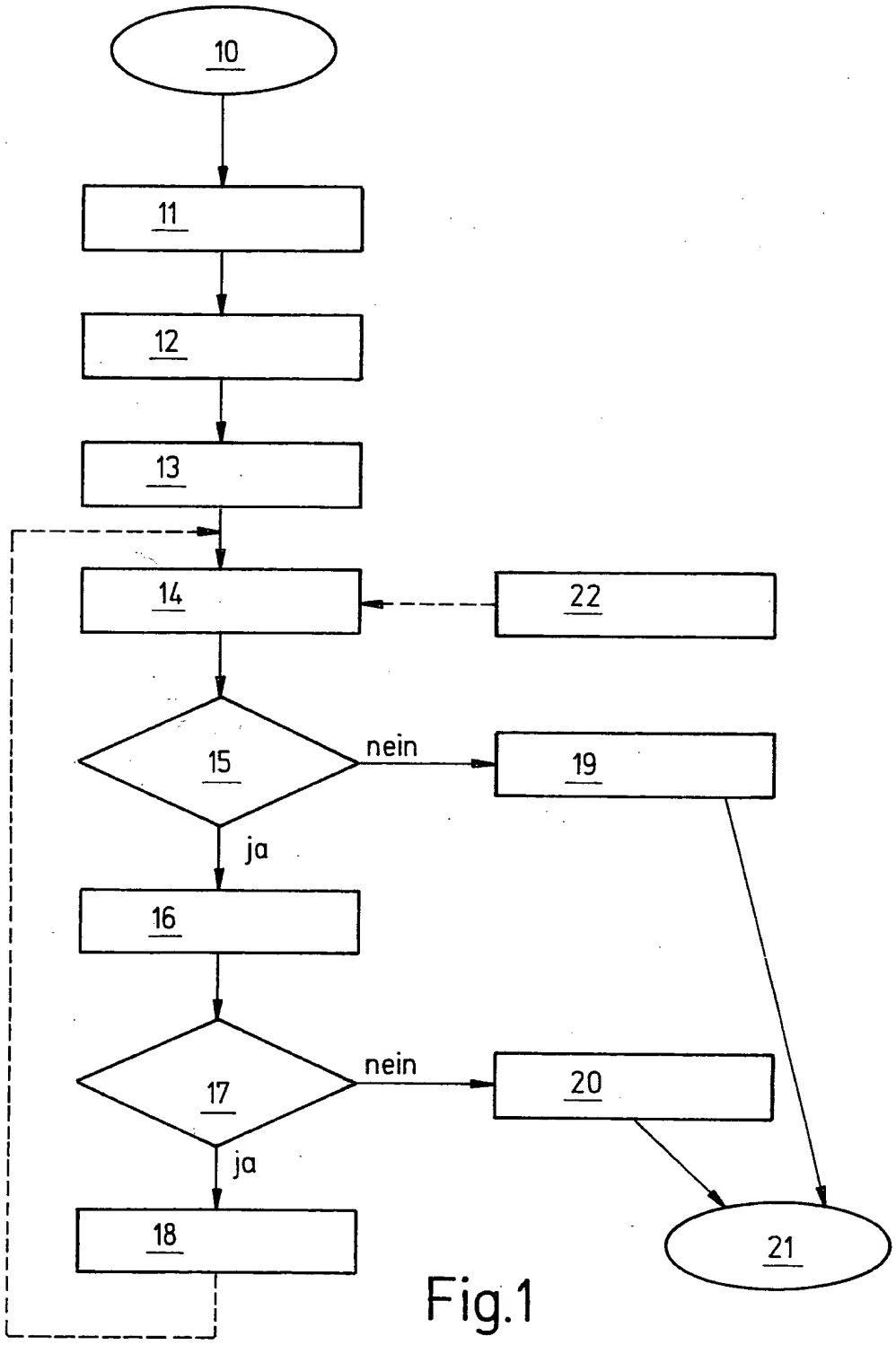

Fig.1

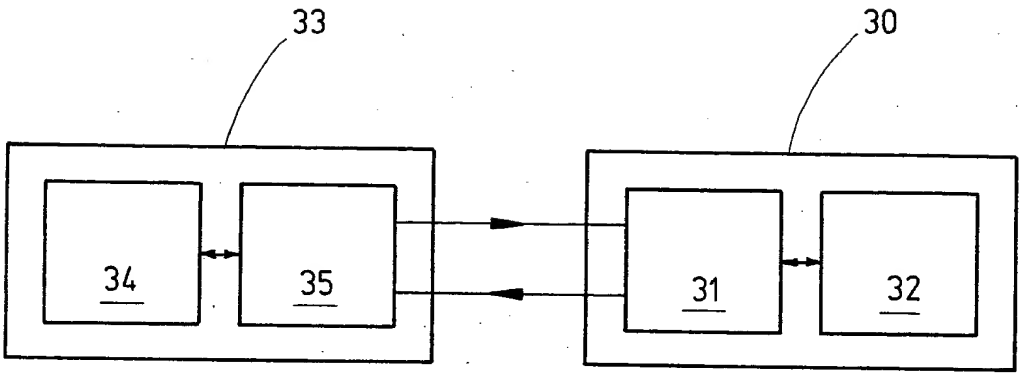

Fig.2